UNCLASSIFIED

AD 409 595

DEFENSE DOCUMENTATION CENTER

FOR

SCIENTIFIC AND TECHNICAL INFORMATION

CAMERON STATION ALEXANDRIA, VIRGINIA

UNCLASSIFIED

63-4-2

AFCRL-63-95

Scientific Report No. 5
Contract AF19(604)-7493
March 1963

• applied • mathematics • •

On the Weights of the Elements of Binary Group Codes

by

L. Calabi and E. Myrvaagnes

Air Force Cambridge Research Laboratories
Office of Aerospace Research
United States Air Force
Bedford, Massachusetts

PARKE MATHEMATICAL LABORATORIES, Inc.
One River Road • Carlisle, Massachusetts

• pml • applied • mathematics • pml •

Scientific Report No. 5
Contract AF19(604)-7493
March 1963

• applied • mathematics • •

On the Weights of the Elements of Binary Group Codes

by

L. Calabi and E. Myrvaagnes

Air Force Cambridge Research Laboratories
Office of Aerospace Research
United States Air Force
Bedford Massachusetts

PARKE MATHEMATICAL LABORATORIES, Inc.
One River Road • Carlisle, Massachusetts

PARKE MATHEMATICAL LABORATORIES, INCORPORATED
ONE RIVER ROAD • CARLISLE, MASSACHUSETTS

Requests for additional copies by Agencies of the Department of Defense, their contractors, and other Government agencies should be directed to the:

DEFENSE DOCUMENTATION CENTER (D.D.C.)
ARLINGTON HALL STATION
ARLINGTON 12, VIRGINIA

Department of Defense contractors must be established for ASTIA services or have their 'need-to-know' certified by the cognizant military agency of their project or contract.

All other persons and organizations should apply to the:

U.S. DEPARTMENT OF COMMERCE
OFFICE OF TECHNICAL SERVICES
WASHINGTON 25, D.C.

A limited number of copies are also available by writing to:

PARKE MATHEMATICAL LABORATORIES, INC.
ONE RIVER ROAD
CARLISLE, MASSACHUSETTS

PARKE MATHEMATICAL LABORATORIES, INCORPORATED
ONE RIVER ROAD • CARLISLE, MASSACHUSETTS

Abstract

Various necessary and sufficient conditions are given for the existence of codes with preassigned weights. Some properties of the weight distribution are deduced.

Table of Contents

Introduction

In our study of the minimal weight that the elements of a k-dimensional binary group code $A(n,k)$ of length n can have, one of us gave [6] an elementary, though long, proof of various existence theorems for binary group codes. We present here these and other similar results, relating and deriving them from a well known theorem. As is often the case, these necessary and sufficient conditions for the existence of codes are not easily applied: indeed they require the use of high speed computers already for small values of n and k. We have been able, however, to derive from them some special cases, and some necessary conditions, of practical utility. These are given in the last section. Further study in this direction would seem justified.

1. Codes with preassigned weight vectors.

Let $x_0, x_1, \ldots, x_i, \ldots, x_{2^k-1}$ be the elements of a group code $A = A(n,k)$. We shall always assume that x_0 is the zero vector; that $x_{2^0}, x_{2^1}, \ldots, x_{2^{k-1}}$ are independent; and that the numeration is so chosen that $\sum_i x_{2^{k_i}} = x_{\sum 2^{k_i}}$, where the first summation is of vectors over the field of two elements. Let W be the column vector whose i^{th} row is w_i, the weight of x_i; notice that $w_0 = 0$ is not in W. W will be called the weight vector of A. More generally, let W be a $(2^k-1) \times 1$ matrix whose elements are strictly positive integers w_i. We will say that W is admissible if it is the weight vector of some code A.

In order to formulate a well known criterion of admissibility we have to introduce the following $(2^k-1) \times (2^k-1)$ matrix C. Its row number 2^k consists, from left to right, of 2^k-1 zeros, followed by 2^k consecutive ones, then 2^k consecutive zeros, then 2^k consecutive ones..., to exhaustion; its row number $\sum_{i=1}^{r} 2^{k_i}$ is the sum mod. 2 of the rows number $2^{k_1}, 2^{k_2}, \ldots, 2^{k_r}$. It is easy to recognize that C is the matrix introduced by MacDonald [1] and used by Fontaine and Peterson [2]. If J denotes the $(2^k-1) \times (2^k-1)$ matrix of all ones, one has [1,2]

$$C^{-1} = 2^{1-k}(2C - J).$$

Theorem 1([1,2,3,7]): W is the weight vector of a code $A(n,k)$ if, and only if

1) $\sum w_i = n \cdot 2^{k-1}$

2) the elements of $N = C^{-1} W$ are all non-negative integers.

If W is the weight vector of A, N is called the modular (representation) vector of A. If n_i is the integer in the i^{th} row of N, and if G is the matrix whose k^{th} row is $x_{2^{k-1}}$, then G has n_i columns which represent in binary form the integer i. In particular then $\sum n_i = n$.

$$
\begin{matrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0
\end{matrix}
$$

The matrix C for $K = 4$.

Letting I denote the $(2^K - 1) \times 1$ matrix of all ones, we can prove:

<u>Theorem 2</u>: W is admissible if and only if there is a matrix N, all the elements of which are non-negative integers, such that

$$3) \quad CW = 2^{K-2} N + (\tfrac{1}{2} \sum w_i) I .$$

Moreover, if 3) is satisfied, letting $n = \sum n_i$ one has $\sum w_i = n \cdot 2^{K-1}$; and then W is the weight vector of a code $A(n, K)$.

To prove that 3) is necessary we use Theor. 1. From 2),

$$N = 2^{2-K} CW - 2^{1-K} JW;$$

but 1) implies $JW = n \cdot 2^{K-1} I = \sum w_i$.

To show that 3) is sufficient, let us first show that 3) implies $\sum w_i = 2^{K-1} \sum n_i$. Remembering that each column of C has exactly 2^{K-1} ones [1], we have

$$JCW = 2^{K-1} JW = 2^{K-1} \sum w_i I ;$$

on the other hand

$$2^{k-2} JN + (\tfrac{1}{2}\Sigma w_i) JI = 2^{k-2}\Sigma n_i I + (\tfrac{1}{2}\Sigma w_i)(2^k - 1) I.$$

Thus 3) implies

$$2^{k-1}\Sigma w_i = 2^{k-2}\Sigma n_i + \tfrac{1}{2}(2^k-1)\Sigma w_i$$

which yields 1) with $n = \Sigma n_i$. Further

$$C^{-1}W = 2^{2-k} CW - 2^{1-k} JW = N + 2^{1-k}\Sigma w_i I - 2^{1-k}\Sigma w_i I = N$$

which is 2); and hence 3) is sufficient. It may be interesting to note that the necessity of 3) follows also from the "mapping theorem" of Assmus and Mattson [4].

If we denote by C_j the j^{th} row of C , 3) can be written

$$C_j W = n_j 2^{k-2} + \tfrac{1}{2}\Sigma w_i \;, \qquad j = 1, 2, \ldots, 2^k - 1.$$

This relation gives a different interpretation to the integers n_j . If W is the weight vector of $A(n,k)$, the weights not added in the sum $C_j W$ correspond to the elements of a subcode (or subgroup) of A that we can denote $A_j(m_j, k-1)$. In fact the i^{th} component of C_j can be considered as the value at x_i of the j^{th} character (with values $0, 1$ instead of $1, -1$). Thus $\Sigma w_i - C_j W$ is the sum of the weights of the elements of A_j ; and hence

$$\Sigma w_i - C_j W = m_j 2^{k-2},$$

but also

$$\Sigma w_i - C_j W = \tfrac{1}{2}\Sigma w_i - n_j 2^{k-2} = (n - n_j) 2^{k-2}.$$

Corollary: With the notation just introduced $n_j = n - m_j$; that is n_j is the difference between the "length" of A and that of A_j .

To introduce the next theorem, observe that 3) is equivalent to the statement: $2C_j W - \Sigma w_i$ is a non-negative multiple of 2^{k-1}, for all j .

<u>Theorem 3:</u> W is admissible if and only if

4) $\sum w_i$ is a multiple of 2^{K-1}

5) $C_j W$ is a multiple of 2^{K-2}, for $j = 1, 2, \ldots, 2^K - 1$

6) $2C_j W \geq \sum w_i$ for $j = 1, 2, \ldots, 2^K - 1$.

Moreover, if 4) - 6) are satisfied and we set $C_j W = a_j 2^{K-2}$, $\sum w_i = n \cdot 2^{K-1}$, $n_j = a_j - n$, then $N = [n_j]$ is the modular and W the weight vector of a code $A(n, K)$.

Notice that 5) and 6) do not imply 4), as the following example shows:

$$W = \begin{bmatrix} 1 \\ 2 \\ 2 \\ 3 \\ 3 \\ 4 \\ 4 \end{bmatrix}, \qquad K = 3 .$$

Similarly

$$W = \begin{bmatrix} 8 \\ 8 \\ 8 \\ 2 \\ 2 \\ 2 \\ 2 \end{bmatrix}, \qquad K = 3$$

shows that 4) and 5) do not imply 6). And finally 4) and 6) do not imply 5) because of the example

$$W = \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \qquad K = 3 .$$

The necessity of 4) - 6) is an immediate consequence of 1) and 3). Conversely, 4) and 5) enable us to write $C_j W = n_j 2^{k-2} + \frac{1}{2} \sum w_i$ and 6) to conclude $n_j \geq 0$. Hence 4) - 6) imply 3). The "Moreover" part of the theorem is now clear.

2. Further modifications of Theorem 1.

It is natural to ask whether the $2^k - 1$ conditions of, say, Theorem 2 are independent and thus all have to be checked. Unfortunately the answer is yes: the second example above fails to satisfy Theorem 2 only for $j = 4$ (and fails to satisfy Theorem 3 only for condition 6) with $j = 4$). Convenient permutations allow us to modify this example so that it fails Theorem 2 for any single given value of j .

In this context, the following result may be of interest:

Proposition 1: Given W , let W' be the $(2^{k-1}-1) \times 1$ matrix consisting of the first $2^{k-1}-1$ rows of W . Then W is admissible if and only if

a) W' is admissible

b) $\sum w_i$ (over W) is a multiple of $2^k - 1$

c) $C_j W$ is a multiple of 2^{k-2} for $2^{k-1} < j \leq 2^k - 1$.

The proof is an immediate consequence of Theorem 3 and of the dependency of C on k as described in [1].

Let us extend the use of a "prime" to differentiate the symbols referring to the subcode generated by the first $k-1$ generators. If $\bar{C}$ denotes the matrix obtained from C by substituting 1 for 0 and 0 for 1, then we know from [1] that

$$G = \left[\begin{array}{c|c|c} C' & \begin{matrix} 0 \\ 0 \\ \vdots \\ 0 \end{matrix} & C' \\ \hline 0\,0 \cdots 0 & 1 & 1\,1 \cdots 1 \\ \hline C' & \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix} & \bar{C}' \end{array}\right]$$

Let C^* denote the matrix obtained from C by substituting 1 for 0 and -1 for 1. Then clearly

$$C^* = \left[\begin{array}{c|c|c} C'^* & \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix} & C'^* \\ \hline 1\,1 \cdots 1 & -1 & -1\,-1 \cdots -1 \\ \hline C'^* & \begin{matrix} -1 \\ -1 \\ \vdots \\ -1 \end{matrix} & -C'^* \end{array}\right]$$

We set

$$H = \left[\begin{array}{c|c} 1 & 1\,1 \cdots\cdots 1 \\ \hline \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix} & C^* \end{array}\right]$$

$$\tilde{W} = \begin{array}{|c|} \hline w_0 \\ \hline W \\ \hline \end{array} \qquad w_0 = 0$$

$$\tilde{N} = \begin{array}{|c|} \hline n_0 \\ \hline N \\ \hline \end{array} \qquad n_0 = -n = -\sum_{i=1}^{2^k-1} n_i$$

$$R = \begin{array}{|c|} \hline w_0 \\ w_1 \\ \vdots \\ w_{2^{k-1}-1} \\ \hline \end{array} \qquad S = \begin{array}{|c|} \hline w_{2^{k-1}} \\ \vdots \\ w_{2^k-1} \\ \hline \end{array}$$

$$T = \begin{array}{|c|} \hline n_0 \\ n_1 \\ \vdots \\ n_{2^{k-1}-1} \\ \hline \end{array} \qquad V = \begin{array}{|c|} \hline n_{2^{k-1}} \\ \vdots \\ n_{2^k-1} \\ \hline \end{array}$$

Then

$$\tilde{W} = \begin{array}{|c|} \hline R \\ \hline S \\ \hline \end{array} \qquad \tilde{W}' = R \qquad \tilde{N} = \begin{array}{|c|} \hline T \\ \hline V \\ \hline \end{array}$$

$$H = \begin{array}{|c|c|} \hline H' & H' \\ \hline H' & -H' \\ \hline \end{array} .$$

Lemma 1: $\widetilde{N}' = T + V.$

Observe that the generator matrix G has n_i columns representing the binary number $1 \leq i \leq 2^{k-1} - 1$, and $n_{2^{k-1}+i}$ columns representing the number $2^{k-1} + i$, and that both types are identical except in the last row, which is the k^th generator. Hence, $n_i' = n_i + n_{2^{k-1}+i}$.

Further,

$$\begin{aligned} n_0' &= -\sum_{i=1}^{2^{k-1}-1} n_i' \\ &= -\sum_{i=1}^{2^{k-1}-1} (n_i + n_{2^{k-1}+i}) \\ &= -\sum_{i=1}^{2^{k-1}-1} n_i - \sum_{i=2^{k-1}+1}^{2^{k}-1} n_i \\ &= n_{2^{k-1}} - \sum_{i=1}^{2^{k}-1} n_i = n_{2^{k-1}} + n_0 , \end{aligned}$$

terminating the proof.

Lemma 2: Condition 3) in Theorem 2 is equivalent to each one of the following:

7) $C^* W + 2^{k-1} N = 0$

8) $H \widetilde{W} + 2^{k-1} \widetilde{N} = 0.$

That 7) and 8) are equivalent is clear. To show that 3) and 7) are equivalent observe that $C^* = J - 2C$. Thus, since $JW = (\Sigma w_i) I$, 7) yields

$$\Sigma w_i I - 2CW + 2^{k-1} N = 0$$

which is, essentially, 3). This proves also the converse.

We can rewrite 8):

$$\begin{array}{|c|c|}\hline H' & H' \\ \hline H' & -H' \\ \hline\end{array}\ \begin{array}{|c|}\hline R \\ \hline S \\ \hline\end{array} + 2^{K-1}\ \begin{array}{|c|}\hline T \\ \hline V \\ \hline\end{array} = 0,$$

obtaining

$$\begin{cases} \alpha) & H'(R+S) + 2^{K-1}T = 0 \\ \beta) & H'(R-S) + 2^{K-1}V = 0. \end{cases}$$

Adding α) and β) yields

$$H'R + 2^{K-2}(T+V) = 0$$

$$H'\tilde{W}' + 2^{K-2}\tilde{N}^{-1} = 0$$

which is 8) for $K-1$. The matrix H is a Hadamard matrix (see, for example, [8]), and hence $H^{-1} = 2^{-K}H$.

Thus β) becomes:

$$H'(S-R) = 2^{K-1}V$$

or

$$S-R = H'V.$$

We have:

Theorem 4: W is admissible if and only if there is a matrix V whose elements are non-negative integers, such that:

a) W' is admissible

b) $S-R = H'V$

c) $\tilde{N}'-V$ is non negative, except in the first row.

The "if" part has been shown above. To prove the "only if" part, assume that a) and b) are satisfied. Retracing the steps above we have

from a) $H'R + 2^{k-2}\tilde{N}' = 0$

and from b) $H'(R-S) + 2^{k-1}V = 0$,

which is β). Subtracting,

$$H'(2R - R + S) + 2^{k-1}(\tilde{N}' - V) = 0$$

or

$$H'(R+S) + 2^{k-1}(\tilde{N}' - V) = 0,$$

which is γ) because of c). But α) and β) give us 8) and hence W is admissible by Theorem 2 and Lemma 2.

Notice that a) and b) do not imply c), as the following example shows. Let

$$W = \begin{bmatrix} 7 \\ 3 \\ 4 \\ 3 \\ 6 \\ 2 \\ 3 \end{bmatrix}, \qquad W' = \begin{bmatrix} 7 \\ 3 \\ 4 \end{bmatrix}.$$

Theorem 2 shows that

$$W' = \begin{bmatrix} 7 \\ 3 \\ 4 \end{bmatrix}$$

is admissible and that the corresponding modular vector is

$$N' = \begin{bmatrix} 4 \\ 0 \\ 3 \end{bmatrix}.$$

By definition

$$R = \begin{bmatrix} 0 \\ 1 \\ 3 \\ 4 \end{bmatrix} \qquad S = \begin{bmatrix} 3 \\ 6 \\ 2 \\ 3 \end{bmatrix}.$$

If we set

$$V = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

then also b) is satisfied: $S - R = H'V$. But c) is not:

$$\tilde{N} - V = \begin{bmatrix} -7 \\ 3 \\ -1 \\ 2 \end{bmatrix}.$$

Theorem 4 has a natural intuitive interpretation which we shall illustrate by an example for $K=3$. Suppose part a) of Theorem 4 is satisfied. That is, there exists a code $A' = \{x_0, x_1, x_2, x_3\}$ with weight vector $W' = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix}$ and modular vector $N' = \begin{bmatrix} n_1 \\ n_2 \\ n_3 \end{bmatrix}$. We wish to determine whether $W = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \end{bmatrix}$ is admissible. The admissibility of W, given that W' is admissible, clearly implies that we can add a generator x_4 to A, satisfying four conditions:

i) the weight of x_4 is w_4,

ii) the weight of $x_5 = x_1 + x_4$ is w_5,

iii) the weight of $x_6 = x_2 + x_4$ is w_6,

and iv) the weight of $x_7 = x_1 + x_2 + x_4$ is w_7.

Let v_i $(i = 0, 1, 2, 3)$ be the number of positions in which x_4 has ones in common with only those generators $x_{2^{\ell_j}}$ such that $i = \sum 2^{\ell_j}$. That is, x_4 has v_0 ones in positions vacant in both x_1, and x_2, v_1 ones in positions common to x_1 but not x_2, v_2 ones in positions common to x_2 but not x_1, and v_3 ones in positions which contain ones in both x_1 and x_2; and this clearly exhausts x_4.

Recalling that $w_0 = 0$, we can translate the four conditions i) - iv) into equations:

$$w_0 + v_0 + v_1 + v_2 + v_3 = w_4$$

$$w_1 + v_0 - v_1 + v_2 - v_3 = w_5$$

$$w_2 + v_0 + v_1 - v_2 - v_3 = w_6$$

$$w_3 + v_0 - v_1 - v_2 + v_3 = w_7 .$$

Collecting the w_i's and setting $V = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{bmatrix}$, we obtain

$$\begin{bmatrix} w_4 - w_0 \\ w_5 - w_1 \\ w_6 - w_2 \\ w_7 - w_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} V.$$

The left-hand member is $S-R$, and the matrix of coefficients of V is H', so this equation is precisely part b) of Theorem 4. The requirement in Theorem 4 that V be of non-negative integers follows here directly from the definition of the v_i. Moreover, since each v_i counts positions from among those counted by the corresponding n_i, it is clear that for $i > 0$, $v_i \leq n_i$, which is part c) of Theorem 4. It can be seen quite easily that these conditions on the v_i are both necessary and sufficient for the admissibility of W. They can be shown by induction to hold for any k. In fact, it was this elementary approach of comparing a new generator with each previous generator that first suggested Theorem 4 to us.

3. Equivalence of weight vectors.

Because of the numeration involved in associating W to a code A, different weight vectors correspond to one and the same code. On the other hand if W is the weight vector of A (with a given numeration), W is also the weight vector of any code equivalent to A. We have thus a "many-to-many" correspondence between admissible vectors W and codes. To obtain a one-to-one correspondence we consider only equivalence classes of codes and equivalence classes of vectors, defined as follows. Two admissible vectors W, W' are called <u>equivalent</u> if they are weight vectors of equivalent codes. The remark above enables us immediately to say also that W and W' are equivalent if and only if they are weight vectors of one and the same code A (for two numerations of its elements).

<u>Proposition 2</u> $W_1 = [w_{1i}]$ and $W_2 = [w_{2i}]$ are equivalent if and only if there is a permutation σ of $\{1, 2, \ldots, 2^k - 1\}$ such that $w_{2i} = w_{1\sigma(i)}$ and such that if $\sigma(2^i) = \sum_{k=0}^{k-1} a_{ik} 2^k$, $a_{ik} = 0, 1$ then $\sigma(\sum_j 2^{i_j}) = \sum_{k=0}^{k-1} (\textstyle\sum\!\!\!\!\!\;\circ_j\, a_{i_j k}) 2^k$, where $\textstyle\sum\!\!\!\!\!\;\circ$ denotes sum modulo 2. It is enough to prove that these properties characterize the changes in allowable numerations of the elements of a code A. Let then $x_1, x_2, \ldots$, $y_1, y_2, \ldots$ denote the elements of A, in two different orders, but such that

$$x_{\sum_j 2^{i_j}} = \sum_j x_{2^{i_j}}, \qquad y_{\sum_j 2^{i_j}} = \sum_j y_{2^{i_j}} .$$

For some permutation σ we have $y_i = x_{\sigma(i)}$.
In particular

$$y_{2^i} = x_{\sigma(2^i)} = x_{\sum_k a_{ik} 2^k} = \sum_k a_{ik} x_{2^k} ;$$

$$x_{\sigma(\sum_j 2^{i_j})} = y_{\sum_j 2^{i_j}} = \sum_j y_{2^{i_j}} = \sum_j \sum_k a_{i_j k}\, x_{2^k} = \sum_k (\textstyle\sum\!\!\!\!\!\;\circ_j\, a_{i_j k}) x_{2^k} = x_{\sum_k (\sum\!\!\!\!\!\;\circ_j\, a_{i_j k}) 2^k} .$$

Conversely, let $x_1, x_2, \ldots$ be an allowable numeration of the elements of A, and let σ have the properties of the proposition. Set $y_i = x_{\sigma(i)}$. To prove that $y_{2^0}, y_{2^1}, \ldots, y_{2^{k-1}}$ are independent, assume $\sum_j y_{2^{i_j}} = 0$. Then

$$0 = \sum_j x_{\sigma(2^{i_j})} = \sum_j x_{\sum_k a_{i_j k} 2^k} = \sum_j \sum_k a_{i_j k} x_{2^k} = \sum_k \left(\sum_j a_{i_j k}\right) x_{2^k} .$$

Since $x_{2^0}, x_{2^1}, \ldots, x_{2^{k-1}}$ are independent, $\sum_j a_{i_j k} = 0$ for each k, and $\sigma(\sum_j 2^{i_j}) = 0$, which is not possible since σ is a permutation. Thus indeed the vectors y_{2^i} are independent.

Moreover

$$y_{\sum_j 2^{i_j}} = x_{\sigma(\sum_j 2^{i_j})} = \sum_j \sum_k a_{i_j k} x_{2^k} = \sum_j x_{\sum a_{i_j k} 2^k} = \sum_j x_{\sigma(2^{i_j})} = \sum_j y_{2^{i_j}} .$$

If we denote by T_σ the $(2^{k-1}) \times (2^{k-1})$ permutation matrix corresponding to the permutation σ of Prop. 2, we can write $W_2 = T_\sigma W_1$. The matrices T_σ so obtained have been denoted P_s in [2]; our Prop. 2 can also be obtained from the definition of P_s. Moreover, in [2] it has been shown that to every σ there corresponds a τ, also with the properties of Prop. 2, such that

$$T_\sigma C = C T_\tau .$$

If then $W_2 = T_\sigma W_1$ and $N = C^{-1} W_1$, $N_2 = C^{-1} W_2$ we obtain

$$N_2 = C^{-1} T_\sigma W_1 = T_\tau C^{-1} W_1 = T_\tau N_1 .$$

This establishes the

Corollary [2] Let A_1, A_2 be two codes, W_1, W_2 and N_1, N_2 their weight and modular vectors. Then the following propositions are equivalent:

a) A_1 and A_2 are equivalent codes;

b) There exists a permutation σ as in Prop. 2 such that
$$W_2 = T_\sigma W_1 ;$$

c) There exists a permutation σ as in Prop. 2 such that
$$N_2 = T_\sigma N_1 .$$

From this one can easily deduce the following almost obvious result:

Proposition 3 Let $N = [n_i]$ be a $(2^k - 1) \times 1$ matrix whose elements are non-negative integers; then N is the modular vector of some code $A(n, k)$ if and only if there exists a permutation σ as in Prop. 2 such that $n_{\sigma(2^i)} \neq 0$ for $i = 0, 1, \ldots, k-1$.

4. Some consequences of Theorems 1 to 4.

Given $W = [w_i]$; let d, d_i be non-negative integers verifying

$$d \leq \min w_i \ , \quad d_i = w_i - d$$

and set

$$D = W - dI = [d_i] \, .$$

In general only the case $d = \min w_i$ will be of interest. However, we need establish the results below also for $d < \min w_i$ so as to obtain more flexibility and, in particular, to be able to use induction arguments. The relations 1) - 7) yield equivalent relations:

1') $\sum d_i - d = (n - 2d)\, 2^k - 1$.

2') the elements of $C^{-1}D + 2^{1-k} dI$ are all non negative integers.

3') $CD = 2^{k-2} N + \tfrac{1}{2} (\sum d_i - d) I$.

4') $\sum d_i - d$ is a multiple of 2^{k-1}.

5') $C_j D$ is a multiple of 2^{k-2} for $j = 1, 2, \ldots, 2^k - 1$.

6') $2 C_j D \geq \sum d_i - d$ for $j = 1, 2, \ldots, 2^k - 1$.

7') $C^* D - dI + 2^{k-1} N = 0$.

Relation 8') and Theorem 4 can also be rewritten in terms of d_i with very little change.

It may be interesting to point out the substitution of $\sum w_i$ with $\sum d_i - d$.

We shall say that (D, d) is admissible if and only if $W = D + dI$ is admissible.

Proposition 4. Let $d_i \neq 0$ for at most two subscripts i_1, i_2. Then (D,d) is admissible if and only if $d+d_{i_1}+d_{i_2}$, $d-d_{i_1}+d_{i_2}$, $d+d_{i_1}-d_{i_2}$ and $d-d_{i_1}-d_{i_2}$ are non negative multiples of 2^{K-1}.

Without loss of generality we can assume $i_1=1$, $i_2=2$ by taking an equivalent weight vector. Then (see the definition of C) $C_1D=d_1$, $C_2D=d_2$, $C_3D=d_1+d_2$, and $C_4D=0$. Moreover all other C_jD have one of these four values.

We can write 3') as

$$-d_1-d_2+d+2C_jD=n_j2^{K-1}.$$

Hence the proposition, which has the known

Corollary The only codes $A(n,K)$ with all elements of equal weight ($d_i=0$ for all i) satisfy $d=k2^{K-1}$, $n=k(2^K-1)$.

Proposition 5 Let $K>3$ and $d_i\neq 0$ only for i_1, i_2, i_3. Then (D,d) is admissible if and only if $d-d_{i_1}+d_{i_2}+d_{i_3}$, $d+d_{i_1}-d_{i_2}+d_{i_3}$, $d+d_{i_1}+d_{i_2}-d_{i_3}$, and $d-d_{i_1}-d_{i_2}-d_{i_3}$ are non negative multiples of 2^{K-1}.

We can reduce the general case to either of two special ones:

a) $i_1=1$, $i_2=2$, $i_3=3$; or b) $i_1=1$, $i_2=2$, $i_3=4$.

In case a), $C_1D=d_1+d_3$, $C_2D=d_2+d_3$, $C_3D=d_1+d_2$, $C_4D=0$ and all other C_jD have one of these values. Our result then follows as above from 3'). In case b) we have $C_3D=d_1+d_2$, $C_5D=d_1+d_4$, $C_6D=d_2+d_4$, $C_7D=0$; hence, again from 3'), the conditions of the proposition are necessary; by a) we know already that they are sufficient. The assumption $K>3$ is required to insure the existence of C_7. Similar results can be obtained for increasing, but always small, number of non-zero d_i's. They can all be considered as particular cases of 7').

The function Σd_i has some interesting properties. The first is a generalization of the Corollary to Prop. 4, which considered the case $\Sigma d_i=0$:

Proposition 6 Let $A(n,K)$ be a code with weights (D,d). Then, for

some integer ℓ, $n = 2\Sigma d_i + \ell(2^{k}-1)$ and $d = \Sigma d_i + \ell\, 2^{k-1}$. Moreover $\ell \geq 0$ if and only if $\Sigma d_i \leq 2^{k-1}$.
From 4') we obtain $d = \Sigma d_i + \ell\, 2^{k-1}$ and then from 1') $n = 2d + \dfrac{\Sigma d_i - d}{2^{k-1}} = 2\Sigma d_i + \ell(2^{k}-1)$. Solving the first relation for Σd_i we obtain $\Sigma d_i = d - \ell\, 2^{k-1}$. Thus $\Sigma d_i \leq 2^{k-1}$ is equivalent to $\ell \geq 0$. Since $n - 2d = -\ell$, we have also:

<u>Corollary</u> $n \leq 2d$ if and only if $\Sigma d_i \leq 2^{k-1}$

The relation $\Sigma d_i \leq 2^{k-1}$ restricts considerably the possible values of Σd_i.

<u>Proposition 7</u> If (D, d) is admissible and $\Sigma d_i < 2^{k-1}$, then $\Sigma d_i = 0$ or $\Sigma d_i = \sum_{\ell=r}^{k-2} 2^{\ell}$ for some $r \geq 0$.

Assume $0 < \Sigma d_i < 2^{k-1}$. Then, for some j, $0 < C_j D \leq \Sigma d_i$. Since $C_j D$ is a multiple of 2^{k-2}, $\Sigma d_i \geq 2^{k-2}$. If the equality sign holds, we are through. Similarly if $C_j D \geq 2^{k-2}$. So assume $C_j D = 2^{k-2} < \Sigma d_i < 2^{k-1}$. We have then $0 < \Sigma d_i - C_j D < 2^{k-2}$. But the middle term is the sum of the d_i's for the subgroup A_j. Using induction we have then

$$\Sigma d_i - C_j D = \sum_{r}^{k-3} 2^{\ell}, \qquad \Sigma d_i = \sum_{r}^{k-2} 2^{\ell}.$$

To complete the proof, let $k = 2$. Then the proposition states $\Sigma d_i = 0, 1$ or $\Sigma d_i \geq 2$: a triviality. Relation 1') yields:

<u>Corollary 1</u>

$$d \leq \left[\frac{n\, 2^{k-1} - 2^{k-2}}{2^{k}-1}\right].$$

This is an improvement on Plotkin's upper bound $\left[\dfrac{n 2^{k-1}}{2^{k}-1}\right]$; however both bounds agree "almost everywhere".
Because of Proposition 6 we obtain also:

<u>Corollary 2</u> If $\Sigma d_i \leq 2^{k-1}$, then $n \geq 2^{k-1}$.

Thus, if $n < 2^{k-1}$, the h of Prop. 6 is strictly negative:

Corollary : If $n < 2^{k-1}$, then $d \leq \left[\frac{n-1}{2}\right]$.

That the values of $\sum d_i$ given in Prop. 7 are actually taken (and then n and d are given by Prop. 6) is shown by the codes described by MacDonald [1] and McCluskey [5], among others.

It is possible to prove, in parallel to Prop. 7, that $\sum d_i = 2^{k-1} + \sum_{i=r}^{k-3} 2^i$ for some $r \leq$ [illegible], if $2^{k-1} < \sum d_i < 2^{k-1} + 2^{k-2}$.

But this result does not seem interesting: the application of Prop. 6 in this case does not determine n and $\sum d_i$ can, and often does, exceed $2^{k-1} + 2^{k-2}$ also for small values of n.

References

1. J.E. MacDonald, Design Methods for Maximum Minimum Distance Error-Correcting Codes, I.B.M.J. 4(1960) p. 43-57.

2. A.B. Fontaine, W.W. Peterson, Group Code Equivalence and Optimum Codes, IRE Trans IT 5(1959) Special Supplement, Trans. 1959 Inter. Symp. Circuit and Information Theory, Los Angeles, Cal., June 16-18, 1959.

3. Slepian, A Class of Binary Signaling Alphabets, B.S.T.J. 35(1956) p. 203-234.

4. E.F. Assmus. H.F. Mattson, Error-Correcting Codes: An Axiomatic Approach, Appl. Res. Lab., Sylvania Electronic Systems, Waltham 54, Mass., ARM No. 269, 27 Sept. 1961.

5. E.J. McCluskey, Error-Correcting Codes, A Linear Programming Approach, B.S.T.J. 38(1959) p. 1485-1512.

6. E. Myrvaagnes, On the Existence of Binary Group Codes with Known Weight Distributions, AF19(604)-7493 TM 5, PML July 1962.

7. N.B. Demidovich, On the Theory of Group Codes, Problemy Kibernetiki No. 5, pp. 105-121, March 1961, abstracted in Automation Express, Vol. 4, no. 7, 1962.

8. R.C. Bose, S.S. Shrikhande, A Note on a Result in the Theory of Code Construction, Inf. + Control, Vol. 2, June 1959, pp. 183-194.

Parke Mathematical Laboratories, Inc.
Carlisle, Massachusetts

On The Weights Of The Elements Of Binary Group Codes

by L. Calabi and E Myrvaagnes

March 1963, 18p. incl. illus
(Scientific Report No 5; AFCRL-63-95)
(Contract AF 19(604)-7493)

Unclassified Report

Various necessary and sufficient conditions are given for the existence of codes with pre-assigned weights. Some properties of the weight distribution are deduced.

UNCLASSIFIED

1. Information Theory
2. Linear Algebra

I. Calabi, L. and E. Myrvaagnes
II. Air Force Cambridge Research Laboratories, Office of Aerospace Research
III. Contract AF19(604)-7493

UNCLASSIFIED

Parke Mathematical Laboratories, Inc.
Carlisle, Massachusetts

On The Weights Of The Elements Of Binary Group Codes

by L. Calabi and E Myrvaagnes

March 1963, 18p. incl. illus.
(Scientific Report No. 5; AFCRL-63-95)
(Contract AF 19(604)-7493)

Unclassified Report

Various necessary and sufficient conditions are given for the existence of codes with pre-assigned weights Some properties of the weight distribution are deduced.

UNCLASSIFIED

1. Information Theory
2. Linear Algebra

I. Calabi, L. and E. Myrvaagnes
II. Air Force Cambridge Research Laboratories, Office of Aerospace Research
III. Contract AF19(604)-7493

UNCLASSIFIED

Parke Mathematical Laboratories, Inc
Carlisle, Massachusetts

On The Weights Of The Elements Of Binary Group Codes

by L. Calabi and E Myrvaagnes

March 1963, 18p. incl illus
(Scientific Report No 5; AFCRL-63-95)
(Contract AF 19(604)-7493)

Unclassified Report

Various necessary and sufficient conditions are given for the existence of codes with pre-assigned weights Some properties of the weight distribution are deduced

UNCLASSIFIED

1 Information Theory
2 Linear Algebra

I. Calabi, L. and E. Myrvaagnes
II. Air Force Cambridge Research Laboratories, Office of Aerospace Research
III. Contract AF19(604)-7493

UNCLASSIFIED

Parke Mathematical Laboratories, Inc.
Carlisle, Massachusetts

On The Weights Of The Elements Of Binary Group Codes

by L Calabi and E Myrvaagnes

March 1963, 18p. incl. illus.
(Scientific Report No. 5; AFCRL-63-95)
(Contract AF 19(604)-7493)

Unclassified Report

Various necessary and sufficient conditions are given for the existence of codes with pre-assigned weights. Some properties of the weight distribution are deduced.

UNCLASSIFIED

1. Information Theory
2. Linear Algebra

I. Calabi, L. and E. Myrvaagnes
II. Air Force Cambridge Research Laboratories, Office of Aerospace Research
III. Contract AF19(604)-7493

UNCLASSIFIED